

## UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of  
 1578 South 67th East Avenue  
 Tulsa, Oklahoma 74112

Case No. 19-mj-218-FHM

**FILED**  
 OCT 16 2019  
 Mark C. McCarthy, Clerk  
 U.S. DISTRICT COURT

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 1029	Fraud and Related Activity in Connection with Access Devices
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1708	Theft of Mail
18 U.S.C. § 1705	Destruction of Letter Boxes or Mail

The application is based on these facts:

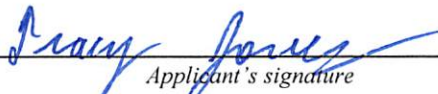
See Affidavit of Postal Inspector Tracy Jones, USPS, attached hereto.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 10-16-19

City and state: Tulsa, OK

  
 Applicant's signature

Postal Inspector Tracy Jones  
 Printed name and title

  
 Judge's signature

Frank H. McCarthy, U.S. Magistrate Judge  
 Printed name and title

**AFFIDAVIT AND STATEMENT OF PROBABLE CAUSE**

I, Tracy Jones, being duly sworn, do hereby depose and state:

1. Your Affiant is Tracy Jones a duly qualified Inspector for the United States Postal Inspection Service (USPIS) who has over 17 years of investigative experience having been so employed by the USPIS since November of 2018. Prior to becoming an Inspector for the USPIS, your affiant was a Special Agent with the Defense Criminal Investigative Service for 1 ½ years, a Special Agent with the United States Postal Service – Office of the Inspector General for 3 years, and a Special Agent with the United States Secret Service for 12 years. Your affiant has received specialized training in the use of the U.S. Mails in narcotics investigations through the USPIS.

2. I am experienced in executing search warrants and debriefing defendants, witnesses, informants, and other persons who have knowledge of specific crimes in violation of the above-mentioned title of the United States Code.

3. Based on my training and experience, I know that individuals who commit financial crimes maintain books, records, receipts, notes, ledgers, bank records, wire transfer receipts, and other papers relating to their clients and/or associates. These items are often maintained where the person has ready access to them such as on his/her person and/or business operations locations.

4. Based on my training and experience, I know that individuals who commit financial crimes maintain records of their correspondence and transactions within their business operations locations. These records may be in the form of written notes and

correspondence, receipts, negotiated instruments, bank statements, and other records.

Records of this kind are often stored on computer (digital) media.

5. Based on my training and experience, I know that individuals who commit financial crimes commonly maintain addresses or telephone numbers of their clients and or associates.

6. Based on my training and experience, I know that individuals who commit financial crimes often utilize cell phones to maintain contact with clients and associates. Furthermore, based on my training and experience, I know that individuals who commit financial crimes often utilize e-mails, text messages, and other communication software to communicate with their clients and/or associates.

7. Based on my training and experience, I know that individuals who commit financial crimes often use electronic devices to maintain records related to the receipt and disposition of the proceeds derived from the fraudulent conduct, including computer software and hardware, CDs, DVDs, thumb drives, and other portable data storage.

8. This affidavit is made in support of an application for a warrant to search the property located at **1578 South 67<sup>th</sup> East Avenue, Tulsa, Oklahoma 74112** (the “**Subject Premises**”), as described in Attachment A. The term “Subject Premises” is meant to encompass the following, to the extent they are located at/on the property known as 1578 South 67<sup>th</sup> East Avenue, Tulsa, Oklahoma 74112: the residential dwelling, vehicles, curtilage, persons, and property such as a computer (as broadly

defined in 18 U.S.C. § 1030(e)(1)) or other digital file storage device located there. This affidavit sets forth facts to establish probable cause to believe that evidence, contraband, fruits, and instrumentalities of illegal activity in violation of, among other statutes, 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1029 (access device fraud), 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1343 (wire fraud), and 18 U.S.C. § 1708 (possession of stolen mail) are currently located at the Premises.

9. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that evidence, contraband, fruits, and instrumentalities of violations of the statutes described above are presently located at the Premises. This affidavit is based on my own personal knowledge, as well as information provided by records, databases and other law enforcement officers.

#### **Probable Cause**

10. On August 19, 2019, a USPS Oklahoma District Incident Report was filed by Station Manager Jeremy Lawson, 6112 East 51<sup>st</sup> Place South, Tulsa, OK 74135. This report documented that 40 Post Office Boxes had been broken into the previous night and an unknown quantity of mail had been stolen. Continuing this same date, Inspector Jones reviewed the surveillance video from inside the Post Office lobby and saw a white female enter the lobby on August 18, 2019 at approximately 10:46 PM. She was dressed in

purple pants, a grey hooded sweatshirt, sunglasses, a mask on the lower part of her face, and was carrying a black bag with a shoulder strap. As soon as the unknown female entered the lobby she went directly to box #35702 and pried open the box with an unidentified tool but did not look in the box or steal anything from inside. A review of the P.O. Box application for this box revealed that it was opened by Hillary Ginn on July 10, 2019. The unknown female is seen breaking into multiple P.O. boxes and stealing an unknown quantity of mail and then exiting the Post Office at approximately 11:12 PM.

11. On September 9, 2019, a USPS Oklahoma District Incident Report was filed by Station Manager Jeremy Lawson, 6112 East 51<sup>st</sup> Place South, Tulsa, OK 74135. This report documented that 2 Post Office Boxes had been broken into sometime between September 7-9 and an unknown quantity of mail had been stolen. Inspector Jones reviewed the surveillance video from inside the Post Office lobby and saw a white female enter the lobby on September 7, 2019 at approximately 9:50 PM. She was dressed in blue shorts, a black shirt, a blue denim jacket, green flip flops, and she had a sleeve tattoo on her left forearm. Immediately upon entering the lobby she went directly to P.O. Box #35702 and used her key to open the box. She then stood on ledge of the wall and reached thru her P.O. box and retrieved mail from surrounding boxes. The unknown female is seen breaking into additional P.O. boxes and stealing an unknown quantity of mail and then exiting the Post Office at approximately 9:55 PM.

12. On September 13, 2019, Kay Sewell, 1909 Whispering Pines Circle, Norman, OK 73072, filed police report #2019-056416 with the Tulsa Police Department regarding a check that had been stolen in the mail. Sewell reported that on September 12, 2019, she was contacted by Allegiance Credit Union, 101 North Robinson Avenue, Suite #210, Oklahoma City, OK 73102, notifying her that check #12681 drawn on checking account #371230, in the amount of \$10,000 had been processed thru her account. Sewell said she mailed check #12681 in the amount of \$264.46 to Sanguine Gas Exploration, P.O. Box 700720, Tulsa, OK 74170 on July 31, 2019. This P.O. box is located at the RW Jenkins Post Office, 6910 South Yorktown Avenue, Tulsa, OK 74136. During this time frame the Jenkins Post Office had multiple P.O. boxes broken into and mail stolen from customers. There are no surveillance cameras at this Post Office. Allegiance Credit Union notified Sewell that the altered check in the amount of \$10,000 was deposited into an account at Western Sun Federal Credit Union, 4620 West Kenosha Street, Broken Arrow, OK 74012. The check was mailed in to Western Sun Federal Credit Union along with 4 other altered checks in the amounts of \$5,000, \$825.00, \$3,289.55, and \$15,000 respectively and were deposited into an account belonging to Hillary Ginn's son, Jeffrey Davis II. Davis II was interviewed by Detective Connor Robinson, Broken Arrow Police Department, after coming into the bank to inquire about a letter he received regarding the attempted deposit. Davis II said he did not mail the checks to the bank and after reviewing copies of the checks he noticed the handwriting appeared to be his mothers,

Hillary Ginn. Davis II said he was concerned because his mother had recently asked him how much money he had in his account at Western Sun and that she tried to give him a check from Church on the Move in his name for medical expenses to cash. Davis II said he believed his mother was lying and did not accept the check from her and did not allow her to cash using his account.

13. On September 14, 2019, a USPS Oklahoma District Incident Report was filed by Station Manager Jeremy Lawson, 6112 East 51<sup>st</sup> Place South, Tulsa, OK 74135. This report documented that 2 Post Office Boxes had been broken into the previous night and an unknown quantity of mail had been stolen. Inspector Jones reviewed the surveillance video from inside the Post Office lobby and saw a white female enter the lobby on September 13, 2019 at approximately 7:19 PM. She was dressed in black pants, a pink shirt, and flip flops. The unknown female also had a small female child with her approximately 2 years of age. She can also be seen getting out of a silver 4-door Sedan in the parking lot. After she enters the Post Office she goes to P.O. Box #35702 and stands on the ledge of the wall and reaches thru the box in an attempt to steal mail from surrounding boxes. She is seen breaking into additional P.O. boxes and stealing an unknown quantity of mail and then exiting the Post Office at approximately 7:45 PM.

14. On September 17, 2019, a USPS Oklahoma District Incident Report was filed by Station Manager Jeremy Lawson, 6112 East 51<sup>st</sup> Place South, Tulsa, OK 74135. This report documented that 11 Post Office Boxes had been broken into the previous

night and an unknown quantity of mail had been stolen. Inspector Jones reviewed the surveillance video from inside the Post Office lobby and saw a white female enter the lobby on September 16, 2019 at approximately 8:02 PM. She was dressed in blue Capri pants, a black shirt, and a blue denim jacket. The unknown female is seen breaking into additional P.O. boxes and stealing an unknown quantity of mail and then exiting the Post Office at approximately 8:36 PM

15. On September 23, 2019, a USPS Oklahoma District Incident Report was filed by Station Manager Jeremy Lawson, 6112 East 51<sup>st</sup> Place South, Tulsa, OK 74135. This report documented that 19 Post Office Boxes had been broken into sometime between September 21-23 and an unknown quantity of mail had been stolen. There was also damage to the mail drop chute inside the lobby and the door of parcel locker #35408 was removed. Inspector Jones reviewed the surveillance video from inside the Post Office lobby and saw a white female enter the lobby on September 22, 2019 at approximately 12:50 AM. She was dressed in purple pants, a black shirt, a white full length cover up with a hood, a dust mask on the lower part of her face, and she was carrying a black bag with a shoulder strap. During the video she removes her hood and a large tattoo is visible above her right breast and lower neck area. The unknown female is seen breaking into additional P.O. boxes and stealing an unknown quantity of mail and then exiting the Post Office at approximately 1:14 AM.

16. Continuing this same date, surveillance video from inside the Post Office lobby showed the same white female enter the lobby again on September 22, 2019 at approximately 9:38 PM. She was dressed in green pants, a pink shirt, a white full length cover up with a hood, a dust mask on the lower part of her face, and she was carrying a black bag with a shoulder strap. She was observed breaking into multiple P.O. boxes and used a 36" grabber tool to retrieve mail from the mail drop chute and tubs of mail located behind the Post Office wall. During the video she went to P.O. Box #35702 and used her key to open the box. She then stood on a ledge of the wall and reached thru her P.O. box and attempted to retrieve mail from surrounding boxes. The unknown female is seen breaking into additional P.O. boxes and stealing an unknown quantity of mail and then exiting the Post Office at approximately 10:50 PM.

17. On October 10, 2019, the Grand Jury, Northern District of Oklahoma, issued a true bill on an indictment charging Ginn with (6) counts of violations of 18 USC 1708 – Theft of Mail and Attempted Theft of Mail, and (6) counts of violations of 18 USC 1705 – Destruction of Letter Boxes and Mail. Subsequent to this indictment an arrest warrant was issued for Ginn on October 10, 2019.

18. On October 16, 2019, Inspectors, Tulsa Police Department, and the Broken Arrow Police Department executed the arrest warrant for Ginn at her residence located at 1578 South 67<sup>th</sup> East Avenue, Tulsa, OK 74112. During the arrest of Ginn and subsequent protective sweep multiple pieces of mail were observed with names and

addresses not associated with Ginn or anyone living at the residence. Specifically, (7) pieces of mail were observed with the following information: Yvonne Earls, 7348 South 68<sup>th</sup> East Avenue, Tulsa, OK 74133; Donald Hull, P.O. Box 690415, Tulsa, OK 74169 (located at the USPS Eastside Station which has had P.O. Boxes broken into numerous times since August 1, 2019) ; Kathy Nix, P.O. Box 35702, Tulsa, OK 74153 (located at the USPS Sheridan Station which has had P.O. Boxes broken into numerous times since August 1, 2019), Bobby McClellan 1578 East 67<sup>th</sup> East Avenue, Tulsa, OK 74112, Vera M. Parcell, 1578 South 67<sup>th</sup> East Avenue, Tulsa, OK 74112, Misty Shaklee, 1578 South 67<sup>th</sup> East Avenue, Tulsa, OK 74112.

19. Based on my training and experience I am familiar with and have investigated cases in which stolen mail was used to apply for and fraudulently obtain credit cards using stolen identities and unauthorized change of address. I believe Ginn is engaged in this unlawful activity.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

20. As described in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including on a cellular phone. Thus, the warrant applied for

would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that Electronic files downloaded to a storage medium can be stored for years at little to no cost. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. When a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

22. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- e. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- f. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions

about how computers were used, the purpose of their use, who used them, and when.

- h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

23. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

24. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard

drive to human inspection in order to determine whether it is evidence described by the warrant.

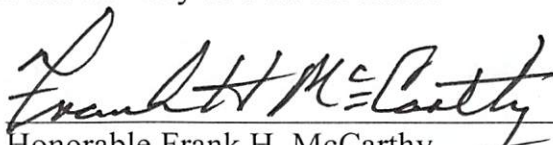
### CONCLUSION

25. Based on the above information, I respectfully submit there is probable cause to believe the Subject Premises described in Attachment A contains evidence of the following violations of Title 18, United States Code: Section 1028A, Aggravated Identity Theft; Section 1029, Fraud and Related Activity in Connection with Access Devices; Section 1341, Mail Fraud; Section 1343, wire fraud; Section 1708, Theft of Mail; and Section 1705, Destruction of Letter Boxes or Mail, among others. The items listed in Attachment B are evidence of these crimes, contraband, fruits of these crimes, or property that is or has been used as the means of committing the foregoing offenses as well as other items illegally possessed.

Therefore, I respectfully request that a search warrant be issued, authorizing the search of the Subject Premises described in Attachment A, and the seizure of the items listed in Attachment B.

  
\_\_\_\_\_  
Tracy Jones  
Inspector  
United States Postal Inspection Service

Sworn and subscribed to before me this 16<sup>th</sup> day of October 2019.

  
\_\_\_\_\_  
Honorable Frank H. McCarthy  
United States Magistrate Judge  
Northern District of Oklahoma

**ATTACHMENT "A"**

**DESCRIPTION OF PLACE TO BE SEARCHED:**

**The Subject Premises:**

**The Premises of 1578 South 67<sup>th</sup> East Avenue, Tulsa, OK 74112:**

Including the subsurface and all dwelling structures, outbuildings, vehicles, and appurtenances thereto;

In the County of Tulsa;

In the Northern District of Oklahoma;

**The physical description:**

The subject premises is a single story duplex with 2 units. It has red brick and yellow siding with a white front door. According to the Tulsa County Assessor's public website the entire duplex is approximately 2,385 square feet and has six bedrooms and four bathrooms.



The search warrant includes the named property and its subsurface and all dwelling structures, outbuildings, storage bins, and vehicles located on the curtilage of the same.

**ATTACHMENT “B”**

Evidence of violations of Title 18, United States Code, Sections 1028A, 1029, 1341, 1343, and 1708, including:

- a. Financial records related to the fraud, including bank account records, bank statements, deposit statements/slips, receipts, ledgers, cash receipt books, checks, checkbooks, canceled checks, check registers, withdrawal slips, wire transfers, and cashier's checks.
- b. Currency, checks, debit and credit cards, and any other financial instruments that could contain proceeds of the fraud.
- c. Mail not in the name and/or address of Hillary Ginn.
- d. Records and information relating to the fraud, including obituaries, change of address forms, credit card applications, and any records containing personal identifying information of the victims.
- e. Computers and digital devices that are capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits or instrumentalities of such crimes, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and devices.
- f. Computers and digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store evidence, contraband, fruits, or instrumentalities of such crimes.

- g. Magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes.
- h. Documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software.
- i. Applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched.
- j. Physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data.
- k. Passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media than can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies.)

The term “computer” as used broadly herein, refers to an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device and includes smartphones.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.